Diese Kopfleiste bitte unbedingt ausfüllen!

Familienname, Vorname (bitte durch eine Leerspalte trennen)

Bereich	Berufsnummer	IHK-Nummer	Prüflingsnummer
7 0	1 2 0 2		
Sp. 1-2	Sp. 3-6	Sp. 7-9	Sp. 10-14

Termin: Mittwoch, 29. November 2023

Abschlussprüfung Winter 2023/24

1202

2 Analyse und Entwicklung von Netzwerken

Fachinformatiker
Fachinformatikerin
Systemintegration

Teil 2 der Abschlussprüfung

4 Aufgaben
90 Minuten Prüfungszeit
100 Punkte

Bearbeitungshinweise

1. Bevor Sie mit der Bearbeitung der Aufgaben beginnen, überprüfen Sie bitte die **Vollständigkeit** dieses Aufgabensatzes. Die Anzahl der zu bearbeitenden Aufgaben ist auf dem Deckblatt links angegeben. Wenden Sie sich bei Unstimmigkeiten sofort an die Aufsicht, weil Reklamationen am Ende der Prüfung nicht anerkannt werden können.
2. Füllen Sie zuerst die **Kopfzeile** aus. Tragen Sie Ihren Familiennamen, Ihren Vornamen und Ihre Prüflings-Nr. in die oben stehenden Felder ein.
3. Lesen Sie bitte den **Text** der Aufgaben ganz durch, bevor Sie mit der Bearbeitung beginnen.
4. Halten Sie sich bei der Bearbeitung der Aufgaben genau an die **Vorgaben der Aufgabenstellung** zum Umfang der Lösung. Wenn z. B. vier Angaben gefordert werden und Sie sechs Angaben anführen, werden nur die ersten vier Angaben bewertet.
5. Tragen Sie die frei zu formulierenden **Antworten dieser offenen Aufgaben** in die dafür lt. Aufgabenstellung vorgesehenen Bereiche (Lösungszeilen, Formulare, Tabellen u. a.) des Arbeitsbogens ein.
6. Sofern nicht ausdrücklich ein Brief oder eine Formulierung in ganzen Sätzen gefordert werden, ist eine **stichwortartige Beantwortung** zulässig.
7. Schreiben Sie deutlich und gut lesbar. Ein nicht eindeutig zuzuordnendes oder **unleserliches Ergebnis** wird als **falsch** gewertet.
8. Zur Lösung der Rechenaufgaben darf ein nicht programmierter, netzunabhängiger **Taschenrechner** ohne Kommunikationsmöglichkeit mit Dritten verwendet werden.
9. Wenn Sie ein **gerundetes Ergebnis** eintragen und damit weiterrechnen müssen, rechnen Sie (auch im Taschenrechner) nur mit diesem gerundeten Ergebnis weiter.
10. Für **Hilfsaufzeichnungen** können Sie das in der Tasche beigelegte Konzeptpapier verwenden. Bewertet werden jedoch grundsätzlich nur Ihre Eintragungen in diesem Aufgabensatz.

Wird vom Korrektor ausgefüllt!

Bewertung

Für die Bewertung gilt die Vorgabe der Punkte in den Lösungshinweisen.

1. Aufg. ☐☐ (15 16) Punkte 2. Aufg. ☐☐ (17 18) Punkte 3. Aufg. ☐☐ (19 20) Punkte 4. Aufg. ☐☐ (21 22) Punkte

Prüfungszeit ☐ (23)
Die entsprechende Ziffer (1, 2 oder 3) finden Sie in der Abfrage nach der Prüfungszeit im Anschluss an die letzte Aufgabe.

Gesamtpunktzahl ☐☐☐ (24 25 26)

Prüfungsort, Datum

Unterschrift

Gemeinsame Prüfungsaufgaben der Industrie- und Handelskammern. Dieser Aufgabensatz wurde von einem überregionalen Ausschuss, der entsprechend § 40 Berufsbildungsgesetz zusammengesetzt ist, beschlossen. Hinweis: Im Interesse einer besseren Lesbarkeit wird in der Aufgabenstellung und in den Angaben zur Aufgabenstellung nur die männliche Form (generisches Maskulinum) verwendet. Die verkürzte Sprachform beinhaltet keine Wertung und die gewählten männlichen Formulierungen gelten uneingeschränkt auch für die weiteren Geschlechter.
Die Vervielfältigung, Verbreitung und öffentliche Wiedergabe der Prüfungsaufgaben und Lösungen ist nicht gestattet. Zuwiderhandlungen werden zivil- und strafrechtlich (§§ 97 ff., 106 ff. UrhG) verfolgt. – © ZPA Nord-West 2023 – Alle Rechte vorbehalten!

Die folgenden Aufgaben 1 bis 4 beziehen sich auf die folgende Ausgangssituation:

Sie arbeiten als Fachinformatiker bei der 1234-IT-Systemhaus GmbH. Für Ihren Arbeitgeber beraten Sie u. a. eine Spedition, die IHK-Transport GmbH. Die Spedition betreibt neben der Zentrale in Berlin noch Filialen in München und Hamburg. Den Netzwerkplan der Spedition finden Sie in der perforierten Anlage

Korrekturrand

1. Aufgabe (21 Punkte)

Die Filialen der Spedition IHK-Transport GmbH sind über statische Routen miteinander verbunden.

a) Auszug aus der Routingtabelle auf Router RB1:

Netz-ID	Subnetzmaske / CIDR	Next-Hop / Interface
10.10.10.0	/28	Eth 0
10.1.1.0	/30	Eth 1
10.2.2.0	/30	Eth 2
172.16.64.0	/22	10.2.2.2
192.168.100.0	/24	10.1.1.2
203.0.113.12	/30	Eth 4
0.0.0.0	/0	203.0.113.14

aa) Die Mitarbeiter der Filiale in Hamburg melden, dass ein Zugang zu den Servern in Berlin nicht möglich ist. Ein Administrator prüft daraufhin die Routingtabelle auf Router RB1.

Welche zwei Fehler in der Routingtabelle sind dafür verantwortlich?

Erläutern Sie, wie das Problem behoben werden kann.

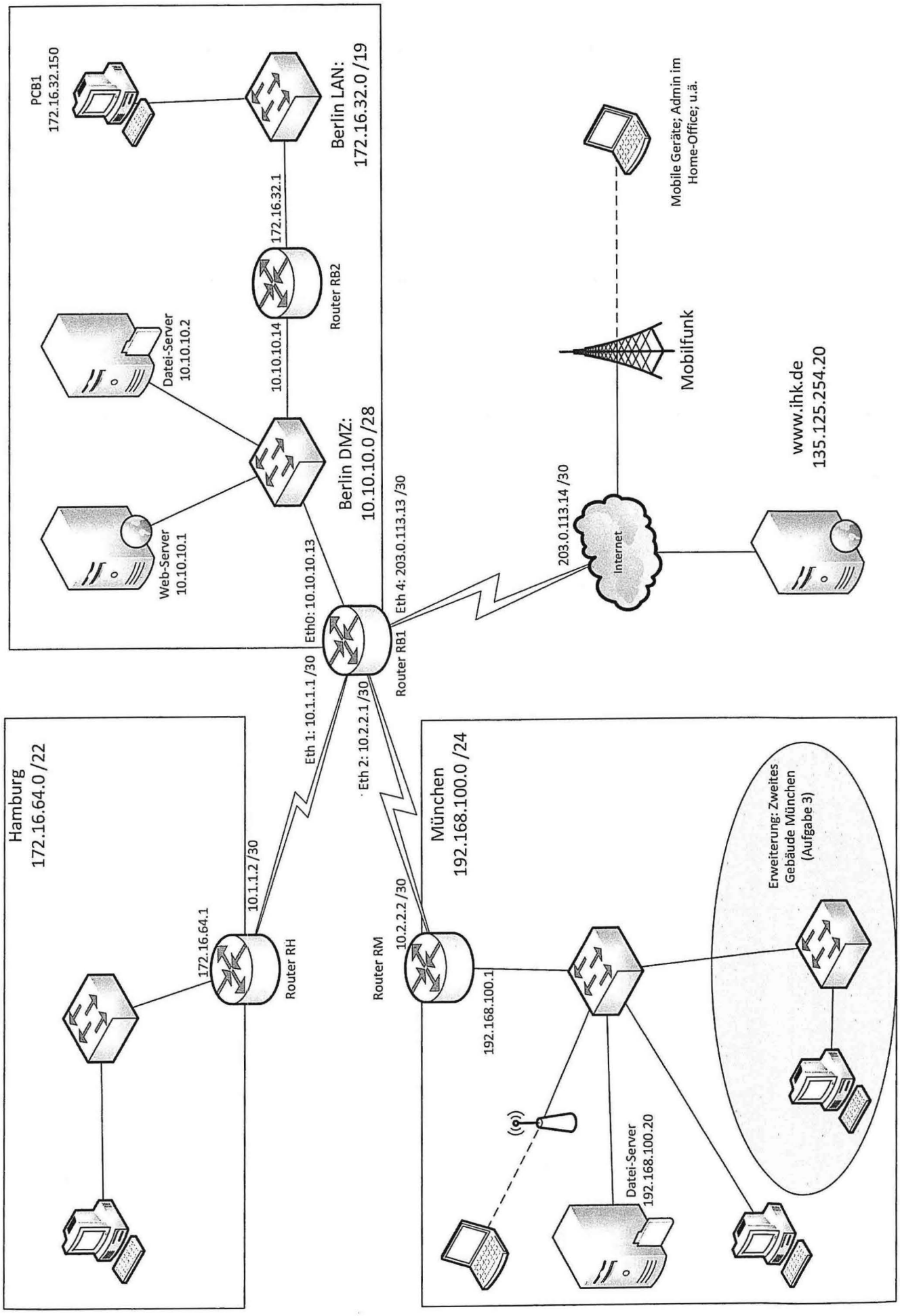
4 Punkte

ab) Beschreiben Sie zwei Vorteile, die dynamische Routingprotokolle gegenüber Netzwerkkonfigurationen mit statischem Routing bieten.

6 Punkte

Dieses Blatt kann an der Perforation aus dem Aufgabensatz herausgetrennt werden!

Anlage 1: Netzwerkplan der IHK-Transport GmbH



Wireshark

Datei Bearbeiten Ansicht Navigation Aufzeichnen Analyse Statistiken Telephonie Wireless Tools Hilfe

Anzeigefilter anwenden … <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
778	243.451794	192.168.100.212	192.168.100.20	ICMP	78	Echo (ping) request id=0x0001, seq=18/4608, ttl=128 (reply in 781)
781	243.452176	192.168.100.20	192.168.100.212	ICMP	78	Echo (ping) reply id=0x0001, seq=18/4608, ttl=64 (request in 778)
784	244.460612	192.168.100.212	192.168.100.20	ICMP	78	Echo (ping) request id=0x0001, seq=19/4864, ttl=128 (reply in 785)
785	244.460612	192.168.100.20	192.168.100.212	ICMP	78	Echo (ping) reply id=0x0001, seq=19/4864, ttl=64 (request in 784)
789	245.473307	192.168.100.212	192.168.100.20	ICMP	78	Echo (ping) request id=0x0001, seq=20/5120, ttl=128 (reply in 790)
790	245.473307	192.168.100.20	192.168.100.212	ICMP	78	Echo (ping) reply id=0x0001, seq=20/5120, ttl=64 (request in 789)
793	246.479617	192.168.100.212	192.168.100.20	ICMP	78	Echo (ping) request id=0x0001, seq=21/5376, ttl=128 (reply in 794)
794	246.479617	192.168.100.20	192.168.100.212	ICMP	78	Echo (ping) reply id=0x0001, seq=21/5376, ttl=64 (request in 793)

```
> Frame 778: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{58E06F70-38E4-4725-85A1-79AB4C68C102}, id 0
> Ethernet II, Src: LiteON_49:9a:f2 (6c:4b:90:49:9a:f2), Dst: Elitegro_62:38:7d (f4:4d:30:62:38:7d)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 11
> Internet Protocol Version 4, Src: 192.168.100.212, Dst: 192.168.100.20
> Internet Control Message Protocol
```

```
0000  f4 4d 30 62 38 7d 6c 4b  90 49 9a f2 81 00 00 0b   ·M0b8}lK ·I····  
0010  08 00 45 00 00 3c a4 c1  00 00 80 01 4b c6 c0 a8   ··E··<·· ····K···
0020  64 d4 c0 a8 64 14 08 00  4d 49 00 01 00 12 61 62   d···d··· MI····ab
0030  63 64 65 66 67 68 69 6a  6b 6c 6d 6e 6f 70 71 72   cdefghij klmnopqr
0040  73 74 75 76 77 61 62 63  64 65 66 67 68 69         stuvwabc defghi
```

VLAN ID (vlan.id), 2 Bytes | Pakete: 812 · Angezeigt: 812 (100.0%) · Verworfen: 0 (0.0%) | Profil: Default

ac) In der Praxis enthält eine Routingtabelle (neben den oben abgedruckten, verkürzten Informationen) noch die sogenannte Metrik oder „Costs".

Erklären Sie die Funktion dieser Angaben für das Routing. 4 Punkte

Korrekturrand

ad) Die Server in der DMZ in Berlin sind aus dem öffentlichen Netz zunächst nicht erreichbar, da sie private Adressen nutzen.

Nennen Sie eine Möglichkeit, wie Sie den Zugriff auf die Server aus dem Internet ermöglichen können. 2 Punkte

b) Die meisten Mitarbeiter der Filiale in München möchten sich in Zukunft auch mit mobilen Endgeräten über WLAN im lokalen Netzwerk anmelden. Für das WLAN soll das Verfahren „WPA2/3-Enterprise" verwendet werden.

ba) Erläutern Sie das Verfahren „WPA2/3-Enterprise". 3 Punkte

bb) Nennen Sie zwei Vorteile dieses Verfahrens gegenüber der Variante mit PSK. 2 Punkte

2. Aufgabe (25 Punkte)

Korrekturrand

a) Die Anbindung der IHK-Transport GmbH an das Internet erfolgt über den Router RB1 in Berlin. Vom Provider hat die Spedition die folgende statische IP-Adresse erhalten: 203.0.113.13 / 30.

aa) Damit die internen Clients der Spedition Daten aus dem Internet abrufen können, muss der Router RB1 in Berlin NAT/PAT ermöglichen.

Erläutern Sie, was man unter NAT und PAT versteht. 4 Punkte

ab) Client PCB1 in Berlin möchte die Seite `https://www.ihk.de/index.html abrufen` (siehe Netzwerkplan).

Vervollständigen Sie die folgenden Ausschnitte aus dem Header auf dem Weg des Pakets. 3 Punkte

IP-Paket auf dem Weg **von Client PCB1 bis zum Router RB2:**

TTL: 128	Protokoll: 06	Header-Checksum: 54466
Quell-IP-Adresse:		
Ziel-IP-Adresse:		
Quell-Port: 49152		Ziel-Port:

ac) Ergänzen Sie den folgenden Ausschnitt aus dem Header. 5 Punkte

IP-Paket auf dem Weg **vom Router RB1 bis zum ISP**:

TTL:	Protokoll:	Header-Checksum: 32187
Quell-IP-Adresse:		
Ziel-IP-Adresse:		
Quell-Port: 50000		Ziel-Port:

ad) Erläutern Sie, weshalb im zweiten Header-Ausschnitt ein anderer Quell-Port als im ersten Header-Ausschnitt verwendet wird. 2 Punkte

Korrekturrand

b) Die DMZ der Spedition am Standort Berlin verwendet statisch vergebene, private IP-Adressen. Administratoren können über Destination-NAT die Server dennoch von außen erreichen.

ba) Ergänzen Sie die folgenden Ausschnitte aus dem Header für eine Verbindung aus dem Internet zum internen Daten-Server per SSH. Der Server soll von extern und von intern jeweils über den SSH-Standardport erreichbar sein. 4 Punkte

IP-Paket, das aus dem Homeoffice des Admins beim Router RB1 der Spedition ankommt:

Quell-IP-Adresse: 62.155.243.193	
Ziel-IP-Adresse:	
Quell-Port:	Ziel-Port:

bb) Ergänzen Sie den folgenden Ausschnitt aus dem Header. 4 Punkte

IP-Paket, nachdem der Router RB1 der Spedition Destination-NAT durchgeführt hat:

Quell-IP-Adresse:	
Ziel-IP-Adresse:	
Quell-Port:	Ziel-Port:

c) Kunden greifen auch über ihre Smartphones oder über ihre Laptops im Mobilfunknetz auf die Webseite der Spedition zu. Die Kunden erhalten im Mobilfunkbereich von Ihrem Provider eine Adresse aus dem Bereich 10.x.x.x (Carrier Grade NAT).

Erläutern Sie, warum der Provider dem Kunden eine solche Adresse zuweist, und nennen Sie einen Nachteil für den Kunden. 3 Punkte

Erläuterung:

Nachteil:

3. Aufgabe (28 Punkte)

Am Standort München der IHK-Transport GmbH wurde ein zweites Gebäude neu errichtet. In jedem der beiden Gebäude wurde ein VLAN-fähiger Switch mit 10 Gbit/s SFP+ Steckplätzen für die UpLinks verbaut. Die beiden Gebäude haben einen Abstand von 150 Meter und sollen verbunden werden. Sie sollen das Netzwerk konfigurieren.

a) Erläutern Sie zwei Gründe für die Verwendung einer Glasfaserverbindung zwischen den beiden Gebäuden anstelle einer Kupferverbindung. 6 Punkte

Fortsetzung 3. Aufgabe →

Fortsetzung 3. Aufgabe

Korrekturrand

b) Das Netzwerk in München soll in VLANs segmentiert werden.

ba) Beschreiben Sie zwei Gründe, die die IHK-Transport GmbH dazu bewogen haben könnten, VLANs zu verwenden. 4 Punkte

bb) Beide Switche sollen so konfiguriert werden, dass gebäudeübergreifende VLANs betrieben werden können.

Geben Sie an, welche Einstellung Sie auf den beiden Geräten vornehmen müssen. 2 Punkte

bc) Beschreiben Sie die Veränderung im OSI-Layer 2, die bei VLAN-Verbindung zwischen zwei Switches stattfindet. 3 Punkte

c) Nach Implementierung der VLANs melden die Mitarbeiter aus dem Neubau in München folgenden Sachverhalt: „keine Verbindung zum Internet möglich; Zugriff auf den Datei-Server im Hauptgebäude München funktioniert".

ca) Sie kontrollieren die IP-Adresse, die Netzwerkmaske (/24) und das Gateway (Internetrouter mit der IP 192.168.100.1). Alle Werte sind richtig eingetragen, und die Verbindung hat vor Einführung der VLANs funktioniert. Sie starten am PC eine Konsole und kontrollieren die Namensauflösung:

```
C:\Users\user15>nslookup www.ihk.de
DNS   request timed out.
      timeout was 2 seconds.
Server:     UnKnown
Address:    192.168.100.1

DNS   request timed out.
      timeout was 2 seconds.
DNS   request timed out.
      timeout was 2 seconds.
DNS   request timed out.
      timeout was 2 seconds.
DNS   request timed out.
      timeout was 2 seconds.
*** Zeitüberschreitung bei Anforderung an UnKnown.
```

Nennen Sie eine mögliche Ursache für diese Ausgabe. 3 Punkte

cb) Sie überprüfen die Verbindung zum Datei-Server (192.168.100.20) mittels eines Ping-Befehls und zeichnen ein Trace des Netzwerkverkehrs zwischen den beiden Switches auf.

Korrekturrand

```
C:\Users\user15>ping 192.168.100.20

Ping wird ausgeführt für 192.168.100.20 mit 32 Bytes Daten:
Antwort von 192.168.100.20: Bytes=32 Zeit<1ms TTL=64
Antwort von 192.168.100.20: Bytes=32 Zeit<1ms TTL=64
Antwort von 192.168.100.20: Bytes=32 Zeit<1ms TTL=64
Antwort von 192.168.100.20: Bytes=32 Zeit<1ms TTL=64

Ping-Statistik für 192.168.100.20:
     Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
     (0% Verlust),
Ca.  Zeitangaben in Millisek.:
     Minimum = 0ms, Maximum = 0ms, Mittelwert = 0ms
```

Das Trace des Netzwerkverkehrs ist beigefügt (siehe Rückseite perforierte Anlage).

Ermitteln Sie die IP-Adresse des Clients. 2 Punkte

cc) Ermitteln Sie die Nummer des VLANs, über das die Verbindung zum Datei-Server stattfindet. 2 Punkte

cd) Beschreiben Sie eine mögliche Fehlerursache des eingangs beschriebenen Problems der fehlerhaften Internetverbindung und machen Sie einen Vorschlag zur Fehlerbeseitigung. 6 Punkte

Fehlerursache:

Fehlerbeseitigung:

4. Aufgabe (26 Punkte)

Korrekturrand

Für die VPN-Verbindungen der Außendienstmitarbeiter erfolgt die Authentifizierung zurzeit über PSK. In Zukunft soll hierzu eine eigene Certificate Authority (CA) nach X.509 eingesetzt werden, welche die notwendigen Client-Zertifikate signiert (self-signed).

a) Erläutern Sie zwei sicherheitsrelevante Vorteile, die für Zertifikate gegenüber PSK sprechen. 4 Punkte

b) Bei der Einrichtung der CA hat ein Mitarbeiter MD5 als Hash-Algorithmus ausgewählt.

ba) Nachdem Ihre VPN-Software Ihnen MD5 als Sicherheitsrisiko anzeigt, finden Sie folgenden Artikel zu MD5:

MD5 Security

The security of the MD5 hash function is severely compromised. A collision attack exists that can find collisions within seconds on a computer with a 2.6 GHz Pentium 4 processor. Further, there is also a chosen-prefix collision attack that can produce a collision for two inputs with specified prefixes within seconds, using off-the-shelf computing hardware.

These hash and collision attacks have been demonstrated in the public in various situations, including colliding document files and digital certificates.

(https://en.wikipedia.org/wiki/MD5 - Auszug)

Erläutern Sie, warum Hashfunktionen in Zertifikaten nach X.509 eine entscheidende Rolle spielen. 4 Punkte

bb) Erläutern Sie den Begriff einer „collision attack" und warum diese Angriffsmöglichkeit ein auf MD5 basierendes Zertifikat unsicher macht. 4 Punkte

Korrekturrand

c) Nachdem mit SHA-256 ein aktuelles Hashverfahren aktiviert wurde, müssen alle Client-Zertifikate neu erstellt und auf den Mitarbeiter-Notebooks eingerichtet werden. Sie sind mit der Aufgabe betraut, dies bei einem Notebook durchzuführen.

Sie senden dem für die CA verantwortlichen Kollegen den Certificate Signing Request (Zertifikats-Anforderungs-Datei) des Clients und erhalten daraufhin eine E-Mail mit folgenden Dateien im Anhang:

Dateiname	Beschreibung
`Client_Cert.crt`	`enthält Zertifikat für Client`
`CA_Cert.crt`	`enthält Zertifikat für CA`
`CA_Private_Key.key`	`enthält private Key der CA`

ca) Beschreiben Sie, welcher Fehler im Umgang mit den Dateien Ihrem Kollegen unterlaufen ist, und welche Sicherheitslücke durch diesen Fehler Ihres Kollegen entstanden ist. 4 Punkte

cb) Beschreiben Sie, was unternommen werden muss, um den Fehler des Kollegen zu korrigieren. 4 Punkte

d) Die von Ihnen verwendete VPN-Software ist so konfiguriert, dass ausschließlich Verbindungen nach TLS1.3 aufgebaut werden. Dieses Protokoll benutzt das sogenannte Diffie-Hellman-Verfahren.

RFC8446 (Auszug)

```
In the Key Exchange phase, the client sends the ClientHello message, which
contains either a set of Diffie-Hellman key shares, a set of pre-shared key
labels, or both.
```

da) Erläutern Sie die Funktion des Diffie-Hellman-Verfahrens beim Verbindungsaufbau. 3 Punkte

db) Erläutern Sie, zu welchem Zweck bei TLS1.3 asymmetrische Verschlüsselung eingesetzt wird. 3 Punkte

bitte wenden!

PRÜFUNGSZEIT – NICHT BESTANDTEIL DER PRÜFUNG!

Wie beurteilen Sie nach der Bearbeitung der Aufgaben die zur Verfügung stehende Prüfungszeit?

[1] Sie hätte kürzer sein können.
[2] Sie war angemessen.
[3] Sie hätte länger sein müssen.

Abschlussprüfung Winter 2023/24
Lösungshinweise

Fachinformatiker/Fachinformatikerin
Systemintegration
1202

2 Analyse und Entwicklung von Netzwerken

Teil 2 der Abschlussprüfung

Allgemeine Korrekturhinweise

Die Lösungs- und Bewertungshinweise zu den einzelnen Handlungsschritten sind als Korrekturhilfen zu verstehen und erheben nicht in jedem Fall Anspruch auf Vollständigkeit und Ausschließlichkeit. Neben hier beispielhaft angeführten Lösungsmöglichkeiten sind auch andere sach- und fachgerechte Lösungsalternativen bzw. Darstellungsformen mit der vorgesehenen Punktzahl zu bewerten. Der Bewertungsspielraum des Korrektors (z. B. hinsichtlich der Berücksichtigung regionaler oder branchenspezifischer Gegebenheiten) bleibt unberührt.

Zu beachten ist die unterschiedliche Dimension der Aufgabenstellung (nennen – erklären – beschreiben – erläutern usw.).

Für die Bewertung gilt folgender Punkte-Noten-Schlüssel:

Note 1	=		100 – 92 Punkte	Note 2	=	unter	92 – 81 Punkte
Note 3	=	unter	81 – 67 Punkte	Note 4	=	unter	67 – 50 Punkte
Note 5	=	unter	50 – 30 Punkte	Note 6	=	unter	30 – 0 Punkte

Die Vervielfältigung, Verbreitung und öffentliche Wiedergabe der Prüfungsaufgaben und Lösungen ist nicht gestattet. Zuwiderhandlungen werden zivil- und strafrechtlich (§§ 97 ff., 106 ff. UrhG) verfolgt. – © ZPA Nord-West 2023 – Alle Rechte vorbehalten!

1. Aufgabe (21 Punkte)

aa) 4 Punkte

Die Gateways zu den Netzen in Hamburg und München sind vertauscht, dies muss korrigiert werden. (Die Ziel-IP 10.1.1.2 muss beim Netzwerk 172.16.64.0 / 22 stehen und die Ziel-IP 10.2.2.0 muss beim Netzwerk 192.168.100.0 / 24 stehen.)

Sinngemäße Antworten sind auch richtig.

ab) 6 Punkte

Wegwahl wird durch das Routing-Protokoll bestimmt
Berücksichtigt im Vergleich zum statischen Routing den kürzesten, kostengünstigsten, schnellsten oder sichersten Weg
Überlastungen, Leitungs- und Knotenausfälle können durch Alternativ-Routen umgangen werden.
u. a.

ac) 4 Punkte

Für jeden Pfad durch das Netzwerk generiert jeder Routing-Algorithmus einen Wert, der als Metrik bezeichnet wird. Dabei ist ein Pfad umso besser, je geringer seine Metrik ist. Anhand dieses Werts sucht der Router die verwendete Route aus.

ad) 2 Punkte

- NAT/PAT (Destination-NAT)
- Portforwarding
- Getunnelte Verbindung mit VPN

Andere Lösungen sind möglich.

ba) 3 Punkte

WPA2/3 Enterprise stellt ein sicheres Authentifizierungsverfahren zur Verfügung und nutzt Protokolle und Standards wie das Extensible Authentication Protocol (EAP) und RADIUS.
Für die sichere Übertragung werden AES und CCMP als Verschlüsselungs- und Authentifizierungsmechanismus verwendet.

bb) 2 Punkte

Vorteile bei Enterprise:

- Für jeden Client lassen sich spezifische Anmeldedaten einrichten
- Logischer Zugang zu VLANs und WLANs möglich
- Ermöglicht unterschiedliche Zugriffsrechte im Netzwerk
- Einfache Sperre eines Accounts nach dem Austritt aus dem Unternehmen
- Logfiles für die Zugriffe der User können personalisiert erstellt werden

Andere Lösungen sind möglich.

2. Aufgabe (25 Punkte)

aa) 4 Punkte

NAT: Änderung der IP-Adresse auf dem Weg des Pakets
PAT: Änderung der Portnummer auf dem Weg des Pakets

ab) 3 Punkte

TTL: 128	Protokoll: 06	Header-Checksum: 54466
Quell-IP-Adresse: 172.16.32.150		
Ziel-IP-Adresse: 135.125.254.20		
Quell-Port: 49152		Ziel-Port: 443

ac) 5 Punkte

TTL: 126	Protokoll: 06	Header-Checksum: 32187
Quell-IP-Adresse: 203.0.113.13		
Ziel-IP-Adresse: 135.125.254.20		
Quell-Port: 50000		Ziel-Port: 443

ad) 2 Punkte
- Der Router wählt für ausgehende Verbindungen jeweils eine neue Quell-Port-Nummer, da intern auch Pakete mit identischer Quell-Port-Nummer bei ihm ankommen könnten.
- Über die Port-Nummern merkt er sich die Zuordnung, sodass er Antworten an den richtigen internen PC weiterleiten kann.

Andere Antworten sind möglich.

ba) 4 Punkte

Quell-IP-Adresse: 62.155.243.193	
Ziel-IP-Adresse: 203.0.113.13	
Quell-Port: beliebiger Wert zwischen 1024 und 65.535	Ziel-Port: 22

bb) 4 Punkte

Quell-IP-Adresse: 62.155.243.193	
Ziel-IP-Adresse: 10.10.10.2	
Quell-Port: beliebiger Wert zwischen 1024 und 65.535	Ziel-Port: 22

c) 3 Punkte
Der Provider versorgt die Kunden im Mobilfunknetz mit privaten IP-Adressen und übersetzt diese bei sich in öffentliche Adressen. Viele Kunden können mit einer einzigen, gemeinsamen IP das Internet nutzen. Nachteil Kunde: die Geräte beim Kunden sind nicht direkt aus dem Internet erreichbar, ggf. doppeltes NAT.

3. Aufgabe (28 Punkte)

a) 6 Punkte
- Bei Kupfer ist die **Reichweite** maximal 100 Meter. Abstand der Gebäude hier 150 Meter. Glasfaser hat eine größere Reichweite. (Multi-Mode ca. 500 bis 1.500 Meter; Single-Mode mehrere Kilometer)
- Höhere Bandbreite bei Glasfaser. Bei Kupferverbindungen sind Bandbreiten über eine Entfernung von 100 Metern nur mit aufwendiger Hardware möglich. Wenn die Bandbreite in Zukunft auf z. B. 40 Gbit/sec erweitert werden sollte, ist dies mit Kupfer nicht möglich. Eine **Glasfaserverbindung** ist bei der späteren Anforderung nach **höherer Bandbreite** zukunftssicherer.
- Glasfaserleitungen sind gegen **EMV-Störungen** unempfindlich. Wenn sich auf dem Leitungsweg größere elektrische Maschinen bzw. oder starke Magnetfelder befinden, wird die Signalübertragung nicht beeinflusst. Starke Magnetfelder können Kupferleitungen direkt beeinflussen bzw. die Signalübertragung stören.
- Glasfaserleitungen leiten keinen Strom. Bei zwei Gebäuden kann der Anschluss an das Stromnetz unterschiedlich erfolgen. Dadurch können die Gebäude auf unterschiedlichem Potenzial liegen. Bei einer Kupferleitung würde sich wegen des unterschiedlichen Potenzials ein Ausgleichsstrom (Brumm-Spannung) bilden. Dieser Strom würde das Signal beeinflussen. Da eine Glasfaserleitung keinen Strom leitet, sind die beiden Gebäude galvanisch getrennt. Eine sogenannte Brumm-Spannung ist durch diese **„Galvanische Trennung"** nicht möglich.
- Glasfaser bietet einen **Schutz vor Überspannung (Blitzschlag)**. Bei einem Blitzeinschlag in einem der beiden Gebäude oder in den Leitungsweg wird die Energie nicht weitergeleitet. Eine Kupferleitung würde die Energie des Blitzschlages auf alle angeschlossenen Geräte weiterleiten und diese in Mitleidenschaft ziehen.

Weitere Lösungen sind möglich.

ba) 4 Punkte
Mehr Sicherheit, da logische Trennung der Netzwerksegmente
Mehr Flexibilität, da neue Netzsegmente leicht erzeugt werden können
Weniger Hardware, da mehrere Netzwerksegmente auf einem Switch/Kabel laufen
Weniger Kosten, da weniger Hardware angeschafft werden muss
Weniger Verkabelung, da mehrere Netzwerksegmente auf einem Switch/Kabel laufen

Andere Lösungen sind möglich.

bb) 2 Punkte
(V)LAN-Verbindungen zwischen den Switches müssen an den UpLink-Ports auf „tagged" eingestellt werden.

Ähnliche Lösungen (herstellerabhängig) sind möglich.

bc) 3 Punkte
Im OSI-Layer 2 wird ein VLAN-Tag eingefügt. (Dies beinhaltet die Kennzeichnung für VLAN und die VLAN-Nummer.)

Ähnliche Lösungen sind möglich.

ca) 3 Punkte
- Keine Antwort vom eingetragenen DNS (192.168.100.1) erhalten
- DNS-Serverdienst (192.168.100.1) ist nicht erreichbar

cb) 2 Punkte
192.168.100.212

cc) 2 Punkte
VLAN 11

cd) 6 Punkte
Fehlerursache:
Client und Router sind in verschiedenen VLANs konfiguriert. Ein Routing zwischen diesen VLANs findet nicht statt.

Andere Lösungen sind möglich.

Fehlerbeseitigung:
- Den Switch-Port des Clients in das gleiche VLAN wie den Internetrouter aufnehmen.
- Ein Routing zwischen den VLAN 11 und den VLAN des Internetrouters konfigurieren.

Weitere Lösungen sind möglich.

4. Aufgabe (26 Punkte)

a) 4 Punkte
- Kann nicht so leicht ausspioniert werden
- Angriffe über Social-Engineering nicht möglich
- Kann an Geräte bzw. Mitarbeiter gebunden werden
- Höhere kryptografische Sicherheit (Schlüssellängen)

Weitere Antworten sind möglich.

ba) 4 Punkte
Beim Signieren eines Zertifikates durch eine CA wird nicht das gesamte Zertifikat signiert (mit dem Private Key der CA verschlüsselt). Es wird lediglich ein Hashwert des Zertifikates gebildet und signiert, der (bei Kollisionsfreiheit) das Zertifikat eindeutig identifiziert.

bb) 4 Punkte
Bei einem Kollisionsangriff (collision attack) ist es möglich, ein gefälschtes Zertifikat zu erzeugen, welches den gleichen Hashwert hat wie das ursprüngliche. Dadurch werden gefälschte Zertifikate nicht als solche erkannt, sondern akzeptiert. MD5 ist anfällig für Kollisionsangriffe.

ca) 4 Punkte
Der private Schlüssel der CA ist an die Mail angehängt worden. Damit ist er nicht mehr privat (geheim), und die gesamte CA ist kompromittiert.

cb) 4 Punkte
Die gesamte CA muss neu angelegt werden bzw. alle Schlüssel der CA müssen neu generiert werden.
Anschließend müssen sämtliche Zertifikate, die von der alten CA signiert wurden, durch neue ersetzt werden.

(Hinweis: sollte nur der erste Schritt genannt werden, gibt es 2 Punkte. Die 2 weiteren Punkte nur, wenn erkannt wurde, dass alle Client-Zertifikate ausgetauscht werden müssen.)

da) 3 Punkte
DH ist ein Verfahren zum Generieren von symmetrischen Schlüsseln über einen offenen Kanal. Es wird von TLS1.3 genutzt, um auf beiden Seiten einen symmetrischen Session-Key zu erzeugen.

db) 3 Punkte
Asymmetrische Verschlüsselung wird bei TLS1.3 ausschließlich zur Authentifizierung bzw. zum Überprüfen der Signaturen der Zertifikate eingesetzt.